'Big data analytics' and processing of health data for scientific research purposes : the British legal framework

Research Protocol by Ian Lloyd

in Glasgow, United Kingdom, 6 April 2018

Contents

1. Overview of the legal framework 3
a. Which laws regulate the processing of health data for research purposes (the current regime, in force till 25 May 2018) 3
b. Revision of the current legal framework under the GDPR 7
c. The national data processing authority 8
2. Transposition of Article 8.4 of Directive 95/46 10
a. Transposition of Article 8.4 of Directive 95/46 10
b. The regime applying to the processing of personal data for health research purposes 11
c. Are there additional specific conditions governing the processing of data for scientific research purposes? 13
d. Formalities prior to processing: the general regime under the current framework 15
3. Further processing of health data (for research purposes): the current regime 16
4. The GDPR's impact on the current regulatory framework for the processing of health data for research purposes 17
a. The impact of the GDPR on the rules applying to processing for research in the field of health 17
b. Modification to the processing authorisation procedure applying to research in the field of health 19
5. Further processing for research purposes under the GDPR 21
6. Health data sources for research purposes 22
a. Sources of data and their regulation 22
b. Application of the national framework to the AEGLE cases 24
1. Type 2 diabetes 24
2. Intensive Care Unit (ICU) 25
3. Chronic Lymphocytic Leukaemia (CLL) 26

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

1. Overview of the legal framework

a. Which laws regulate the processing of health data for research purposes (the current regime, in force till 25 May 2018)

As discussed below, the bulk of medical care in the UK is provided under the auspices of the National Health Service. Under the devolved system of government in the country, separate provision is made for England, Wales, Scotland and Northern Ireland. These tend to apply at an administrative rather than a regulatory level. Reference to specific provisions in this report will be made with reference to the system applying in England which is the largest jurisdiction within the United Kingdom. It should also be noted that much medical research is funded by charities (such as the Nuffield Foundation and Wellcome Trust) that may make conformity with policies regarding confidentiality a contractual term of any grant.

The Data Protection Act 1998

This legislation is described as "An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information." It is the key legal measure applying in respect of the processing of all kinds of personal data although in the field of health data it tends to establish general principles that are expanded in other items of legislation or regulation. The 1998 Act replaces a previous Act of the same name that was adopted in 1984 and is scheduled itself to be repealed and replaced by the Data Protection Act of 2018, a measure intended to comply with the provisions of the GDPR so as to allow the UK to secure a finding of adequacy from the European authorities subsequent to its departure from the Union.

The Human Rights Act of 1998

.The Human Rights Act of 1998 imposes a requirement on the Government to ensure respect for private life as defined in the European Convention on Human Rights providing in section 6 that:

It is unlawful for a public authority to act in a way which is incompatible with a Convention right.

This is an important provision for the UK given that the National Health Service (NHS), which is classed as a public authority, delivers a large majority (around 80%) of all medical treatment Perhaps more significant for data sharing implications, almost all serious medical treatment and those which might be the subject of data sharing is conducted within the NHS.

The Medical Act 1983

The Medical Act of 1983 (as amended) is the statute that enshrines the General Medical Council (GMC) as the organisation that controls entry to the medical profession and establishes standards of practice that are to be observed by doctors in the course of their work. Section 35 of this Act provides that:

The powers of the General Council shall include the power to provide, in such manner as the Council think fit, advice for members of the medical profession on -

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

(a) standards of professional conduct;

(b) standards of professional performance; or

(c) medical ethics.

Extensive guidance has been produced on the topic of patient confidentiality with the most extensive policy formulation being Confidentiality: good practice in handling patient information which was most recently revised in 2017 and sets out a set of 8 principles that must be complied with by any medical practitioner handling personal data. Such persons are instructed to:

(a) **Use the minimum necessary personal information**. Use anonymised information if it is practicable to do so and if it will serve the purpose.
(b) **Manage and protect information**. Make sure any personal information you hold or control is effectively protected at all times against improper access, disclosure or loss.
(c) **Be aware of your responsibilities**. Develop and maintain an understanding of information governance that is appropriate to your role.
(d) **Comply with the law**. Be satisfied that you are handling personal information lawfully.
(e) **Share relevant information for direct care** in line with the principles in this guidance unless the patient has objected.
(f) **Ask for explicit consent** to disclose identifiable information about patients for purposes other than their care or local clinical audit, unless the disclosure is required by law or can be justified in the public interest.
(g) **Tell patients** about disclosures of personal information you make that they would not reasonably expect, or check they have received information about such disclosures, unless that is not practicable or would undermine the purpose of the disclosure. Keep a record of your decisions to disclose, or not to disclose, information.
(h) **Support patients to access their information**. Respect, and help patients exercise, their legal rights to be informed about how their information will be used and to have access to, or copies of, their health records.
(i) Failure on the part of a doctor to comply with the requirements of the GMC will expose them to a range of sanctions up to and including their entitlement to practice as a medical doctor.

Common and statutory obligations of confidentiality

Given the location of the NHS within the public sector, many aspects of its operations are conducted on the basis of administrative orders rather than formal legal instruments.

Caldicott Guardians

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

Three reviews of patient information handling in the NHS have been conducted by Dame Caldicott. In 1997 on the Review of patient Identifiable Information, in 2013 on Information Governance and in 2016 on, Data Security, Consent and Opt-Outs. These provide the basis for NHS policy and practice regarding the handling of personal data. It is also policy that each Hospital area should appoint a, so called, “Caldicott Guardian”, who will be responsible for ensuring that the standards regarding information handling will be observed within the medical facilities contained within their area of responsibility.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The NHS Act 2006

On occasion, researchers require specific information about individuals that cannot fully be anonymised or pseudonymised, and gaining explicit consent from every individual concerned may not be a feasible option. Section 251 of the 2006 Act provides that:

The Secretary of State may by regulations make such provision for and in connection with requiring or regulating the processing of prescribed patient information for medical purposes as he considers necessary or expedient—

(a) in the interests of improving patient care, or

(b) in the public interest.

(2) Regulations under subsection (1) may, in particular, make provision—

(a) for requiring prescribed communications of any nature which contain patient information to be disclosed by health service bodies in prescribed circumstances—

.

Regulations made under the Act allows the common law duty of confidence to be set aside under specific circumstances. Any powers may only provide relief from the common law duty of confidence. Actions must still comply in full with the requirements of the Data Protection Act. No regulations have been made under the 2006 Act although one set of measures made under identical provisions in the Health and Social Care Act of 2001 remain in force. The Health Service (Control of Patient Information) Regulations 2002 provide in Regulation 2 that:

… confidential patient information relating to patients referred for the diagnosis or treatment of neoplasia may be processed for medical purposes approved by the Secretary of State which comprise or include

(a) the surveillance and analysis of health and disease;

(b) the monitoring and audit of health and health related care provision and outcomes where such provision has been made;

(c) the planning and administration of the provision made for health and health related care;

(d) medical research approved by research ethics committees;

(4) Where the Secretary of State considers that it is necessary in the public interest that confidential patient information is processed for a purpose specified in paragraph (1), he may give notice to any body or person who is approved and authorized under paragraph (3) to require that body or person to process that information for that purpose

By Regulation 4 it is provided that:

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Anything done by a person that is necessary for the purpose of processing confidential patient information in accordance with these Regulations shall be taken to be lawfully done despite any obligation of confidence owed by that person in respect of it.

NHS Digital

The NHS Digital Service was established under the Health and Social Care Act 2012.Section 250 of this Act provides a legal basis for the collection of data by the National Health Service Commissioning Board:

(1)The Secretary of State or the National Health Service Commissioning Board (referred to in this Chapter as "the Board") may prepare and publish an information standard.

(2)For the purposes of this Part "an information standard" is a document containing standards in relation to the processing of information.

Section 252 continues to provide that:

There is to be a body corporate known as the Health and Social Care Information Centre (referred to in this Chapter as "the Information Centre")

Now operating under the trading name NHS Digital, the Information Centre has a wide range of responsibilities. The most relevant task in the present context is to establish information systems for the collection and analysis of specified categories of medical information as directed by the Secretary of State and by a number of other specified stakeholders.. This has been a source of difficulty for the UK. In 2014 the Care.data programme was announced by the NHS. This was to have established a single database containing all patient data that would have been made freely available to researchers in anonymous format and to authorised researchers in a form that would have identified individual patients. Although patients would have enjoyed a limited ability to object to their data being included in the data base, this would have extended only to records generated by general practitioners (rather than hospitals) and held other that in anonymous format. Largely due to data protection concerns and in particular because of concern at the potential implications of the GDPR, this scheme was cancelled at considerable financial cost in 2016 following a review conducted in 2016 by Dame Fiona Caldicott, who holds the office of National Data Guardian. The Office was established by a decision of the Department of Health and is described in the following terms

The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly.

Shared electronic health records are indirectly relevant in this context because they can potentially be an important source for health-related research.

The patient's (electronic) medical file:

Electronic Patients Records

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Within the primary care sector, the NHS makes use of a commercially produced IT system called system referred to as Systmone in order to maintain patient records. Information about the system and the patient's right to opt out of inclusion can be found here. Operation of the system has proved to be somewhat controversial due largely to concerns expressed by the Information Commissioner "about SystmOne's enhanced data sharing function and the potential risk to patients' medical records held by GPs." The operation of the system was the subject of a complaint to the ICO who investigated but concluded that the system was not incompatible with data protection requirements:

Following detailed discussions between the ICO, TPP, NHS Digital and NHS England, TPP has now identified some changes which are intended to address the ICO's concerns about the fair and lawful processing of patient data on the system as well as concerns about the security measures in place to prevent inappropriate access to patient data.

These changes, which will be implemented for GP practices using the system along with updated documentation, are welcome and represent significant progress in addressing the concerns raised by the ICO for GP data controllers using SystmOne.

The ICO will continue to work with TPP and other stakeholders to address any remaining concerns.

This statement represents the situation under the Data Protection Act 1998. The GDPR imposes stricter requirements upon data controllers and it may be that a different result will apply under the new legislation.

Computer Misuse Act 1990

The 1990 Act establishes a number of offences relating to the unauthorised access to and use of data held on a computer system. These are applicable regardless of the nature of the data involved but will certainly be relevant within a health context. Three offences are established in the legislation: the act of seeking to obtain unauthorised access to programs held on a computer, the commission of such an act with the intention of using access to further the commission of a further serious offence (for example seeking to obtain medical data with the intention of blackmailing the data subject) and the act of seeking to cause an unauthorised modification, perhaps following the dissemination of a virus, of the contents of a computer system.

b. Revision of the current legal framework under the GDPR

Implementation of the GDPR has proved to be a complex task. It is accepted by all major political parties that the UK's data protection law should seek to be accepted as adequate by the EU following the UK's departure from the Union in order to protect significant areas of activity such as financial services that are heavily dependent upon the unrestricted flow of personal data. To achieve this, a Data Protection Bill was introduced in the UK Parliament in Autumn 2017 and is expected to become law by May 2018.

The Bill is a substantially larger document than the GDPR, around twice its length. When in force, it will replace the existing data protection legislation. Drafting of the new legislation has been complicated by the Brexit process. As indicated, the need to secure a finding of adequacy has been widely accepted. The UK legislation makes extensive reference to the GDPR but rather than relying upon the direct application of the Regulation, it treats it in many respects as akin to a Directive and seeks to transpose its requirements into the national law.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Apart from the need to ensure acceptance of adequacy for the new law, there has also been a significant change in governmental perception of the importance of data protection legislation. Previous statutes were introduced with a degree of reluctance and sought to enact the bare minimum necessary to comply with international obligations. A series of high profile data mishaps has brought realisation of the importance of the topic and the new measure has received more significant governmental support than its predecessors. The major change that the Bill will introduce that is likely to impact upon medical research is the need for a data processor to secure positive concern from data subjects. Although there will remain exceptions to the principle, these are more stringently defined that has previously been the case.

c. The national data processing authority

Can you provide a short description of the role of the data protection supervisory authority in your country in the domain of processing health data for research purposes under the current legal framework?

In the United Kingdom the Information Commissioner – who in legal terms has the status of a corporation sole, a device intended to provide for a high degree of independence from day to day governmental control – is the supervisory authority in the data protection field.

The general functions of the Commissioner are laid down in Part VI of the 1998 Act. Section 51 provides that *inter alia*:

(1) It shall be the duty of the Commissioner to promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers

(2) The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the public about the operation of this Act, about good practice, and about other matters within the scope of his functions under this Act, and may give advice to any person as to any of those matters

In order to exercise these functions, a range of enforcement powers are conferred on the Commissioner including those of ordering the cessation of illegal processing and the imposition of monetary penalties. Provision is made also for the utilisation of investigatory powers.

The Commissioner is obliged to submit an annual report on her activities to Parliament and is also charged with developing codes of practice relating to particular areas of processing activities either at her own discretion or as required by the Secretary of State.

Can you describe the adopted or proposed changes to this role of the national data protection authority to ensure compliance with the GDPR?

The Commissioner's existing powers and duties essentially continue under the new regime although some significant additional functions and powers are added.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The Commissioner is to be the supervisory authority in the United Kingdom for the purposes of Article 51 of the GDPR. In a number of respects, powers conferred and duties imposed on the Commissioner are increased. Of particular relevance to the present topic might be noted the provisions of the Bill which require that the Commissioner draw up a code of practice relating to data sharing. It is provided that the code is to contain

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation,

and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

Although the code is to be drafted by the Commissioner, it will enter into force only when approved by a Government Minister. In terms of its legal status, a failure on the part of a person to comply with its terms will not itself give rise to liability but may be taken into account in deciding where there has been any breach of the legislation. The Commissioner may be required by a Minster to draft codes in respect of any other form of processing carried out under the legislation

The Commissioner has power to conduct consensual audits of a data controller's activities to determine:

whether the controller or processor is complying with good practice in the processing of personal data.

It is further provided that:

good practice in the processing of personal data" means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, including compliance with the requirements of the data protection legislation;

At the level of compulsion, provision is made for the service of assessment notices that require the Commissioner be allowed to conduct an assessment to determine whether a controller or processor is complying with the data protection legislation. The notice may include terms empowering the Commissioner to enter premises and view any information held therein. Failure to comply with the terms of an assessment notice may expose the controller to a monetary penalty to be levied by the Commissioner. The Commissioner is obliged under the Bill to publish guidance indicating how these powers will be exercised.

In June 2016, the Review of Data Security Consent and Opt-Outs conducted by Dame Fiona Caldicott as part of her review on information handling in the NHS recommended that the Government should criminalise the deliberate re-identification of individuals whose personal data is contained in anonymised data. On 1 March 2017, the Government published the UK Digital Strategy and committed to create a new offence along these lines. The Data Protection Bill provides for such an offence. Section 171 provides that:

It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

2. Transposition of Article 8.4 of Directive 95/46

Did your national legislator insert any additional exemptions for the processing of health data for research purposes? How is it/are they formulated? Please explain. Are there additional exemptions issued by the DPA?

a. Transposition of Article 8.4 of Directive 95/46

Transposition of the Directive is a fairly complex process that requires reference to a number of provisions in the Data Protection Act. The approach is driven in part by the special status afforded to the NHS and there is limited specific reference to the treatment of health data.. Schedule One of the 1998 Act sets out the data protection principles that must be followed by any party processing personal data. It requires that

Personal data shall be processed fairly and lawfully

The term personal data is defined in section one of the Act as:

data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller …

And continues to provide that personal data shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The term "Sensitive personal data" is defined in section 2 as encompassing any information relating to a range of racial, political and other factors, including most relevantly for present purposes::

(e) his physical or mental health or condition,

These requirements are cumulative but Schedule 3 is of the most direct relevance to the present topic. It legitimizes processing where:

1. The data subject has given his explicit consent to the processing of the

personal data.

..

8.—(1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services….

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

The term "health professional" is defined in section 69 of the Data Protection Act as including registered medical practitioners and members of a range of other medical professions and also scientists employed by a "health service body", a concept that applies to organisations constituting part of the NHS (section 70).

The notion of "consent" has posed difficulties for the UK's data protection regime. Traditionally, data protection law has tended to favour an "opt out" system whereby consent to processing will be implied unless the individual gives notice of objection. Even the notion of explicit consent has not been considered as completely incompatible with that of "opt out".

b. The regime applying to the processing of personal data for health research purposes

Is there a specific regime applying to data processing for research in the field of health purposes?

There is no specific regime regarding the processing of personal data for health purposes although such activities are covered by the general data protection regime.

All health and adult social care organisations must, by law, share information with each other about patients they are caring for directly, to improve the care provided. The Health and Social Care (Safety and Quality) Act 2015 which aimed to reduce public anxiety about data sharing[1] requires use of a patient's NHS number (a unique personal identifier) as a consistent identifier when sharing data or information about them. Section 2 of the Act imposes an obligation on the Secretary of State to make regulations giving effect to this provision. To this end the Health and Social Care Act 2012 (Consistent Identifier) Regulations 2015 were made mandating the use of what is referred to as the "NHS number". This is defined as:

[1] The 2013 Caldicott Review found that in some cases this anxiety meant patient information was not shared, even when sharing would have been in the best interest of the patient.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the number, consisting of 10 numeric digits, which serves as the national unique identifier used for the purpose of safely, accurately and efficiently sharing information relating to a registered patient across the whole of the health service in England

It is further provided, however, that data sharing

does not permit the relevant person to do anything which, but for this section, would be inconsistent with—

(a)any provision made by or under the Data Protection Act 1998, or

(b)a common law duty of care or confidence.

Different and in many respects more difficult issues apply when the data sharing moves outside the health service to encompass other partners. A situation that has created considerable controversy has concerned agreements between the artificial intelligence system,, Deep Mind, which is owned by Google and various sectors of the NHS. The aim is to develop clinical tools that use artificial intelligence to provide clinical advice and support. Effectively, the collaboration involves hospitals supplying raw patient data to the company in order to develop applications. One such agreement between Deep Mind and a London hospital drew criticism from the Information Commissioner on the ground that insufficient steps had been taken to secure patient consent to the data sharing.

From which generally applicable data protection provisions are researchers exempted and under what conditions?

The main exception offered to researchers concerns the requirement to seek consent for the processing of personal data. The exception is narrowly defined. NHS Information Governance Guidance published on Legal and Professional Obligations relating to medical research[2] provides that:

If identifiable information must be used, and consent is genuinely not practicable, then in England and Wales, approval may be obtained from the Secretary of State for Health under Section 251 of the National Health Service Act 2006, on the recommendation of the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA). CAG1 provides independent expert advice on the appropriate use of confidential information. It reviews applications for the use of person-identifiable information for research and other secondary purposes, and advises the HRA on whether the use is sufficiently justified. Its key purpose is to protect and promote the interests of patients and the public whilst at the same time facilitating appropriate use of confidential information for purposes beyond direct care.

If you intend to access confidential patient information without consent in England and Wales you should apply to the Confidentiality Advisory Group (CAG).

[2] Available from < file:///Users/ianlloyd/Downloads/NHS-information-governance-legal-professional-obligations%20(2).pdf>

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

c. Are there additional specific conditions governing the processing of data for scientific research purposes?

What are the suitable safeguards applied to the exemption foreseen by Article 8.4 of the Directive in your country?

Paragraph 8 of Schedule 3 of the 1998 Act provides an exemption from the general prohibition against the processing of personal data in the situation where:

(1) The processing is necessary for medical purposes and is undertaken

by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which

is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

The term "health professional is defined in section 69 of the Act to encompass a wide range of medical and related professions:

(a) a registered medical practitioner,

(b) a registered dentist as defined by section 53(1) of the Dentists Act 1984,

(c) a registered optician as defined by section 36(1) of the Opticians. Act 1989,

(d) a registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act 1954 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976,

(e) a registered nurse, midwife or health visitor,

(f) a registered osteopath as defined by section 41 of the Osteopaths. Act 1993,

(g) a registered chiropractor as defined by section 43 of the Chiropractors Act 1994,

(h) any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends,

(i) a clinical psychologist, child psychotherapist or speech therapist,

(j) a music therapist employed by a health service body, and

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

(k) a scientist employed by such a body as head of a department.

(2) In subsection (1)(a) "registered medical practitioner" includes any

person who is provisionally registered under section 15 or 21 of the

Medical Act 1983 and is engaged in such employment as is mentioned in

subsection (3) of that section

The Act contains no provision for additional safeguards when data is processed in reliance on this provision although, as indicated in the section, any person relying upon it will be subject to the operation of professional rules regarding the maintenance of confidentiality.

Are there any specific provisions concerning: (i) professional secrecy, (ii) express consent for specific data, or specific provisions for (iii) deceased data subjects, or (iv) specific provisions for minors or persons subject to guardianship?

The Access to Health Records Act 1990 provide rights of access to a deceased patient's personal representative and any person who may have a claim arising out of a patient's death. Where an application is made by a person who may have a claim, access to patient records is limited to information of relevance to the claim.

Access should be limited or refused if there is evidence:

- that the patient would have expected that the information would not be disclosed to the applicant
- if disclosure is likely to cause serious harm to anyone else, or
- if it would also disclose information about a third party (other than a healthcare professional involved in the deceased person's care) who does not consent.

Access must be refused to records that contain a note, made at the patient's request, expressing that they did not wish access to be given on an application under the Act.

Are there specific requirements about the data subject's information or about the person from whom the data was collected?

Where data is supplied by or collected from an individual, it will be subject to obligations of confidentiality. Additionally and more specifically, the Data Protection Act imposes obligations on a data controller to maintain appropriate levels of security whilst the Computer Misuse Act provides for criminal penalties to be imposed upon persons who secure unauthorised access to personal data. A number of prosecutions have been brought in respect of health data. It appears to be a common fact that the access to attempted or secured by an employee making unauthorised use of authorised access than by an external hacker.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Are there specific penalties if the conditions for processing for scientific research in the field of health purposes are not respected? What do those penalties entail?

The Information Commissioner reports 17 instances of sanctions being imposed upon organisations and/or individuals in respect of the processing of personal health data in breach of requirement imposed under the Data Protection Act and also a number of other statutes. A number of prosecutions have, for example, been brought against (invariably former) NHS employees alleging that they obtained unauthorised access to computer held data. Perhaps more significantly, undertakings have been sought from a number of NHS agencies. The notion of undertakings has been developed by the Commissioner over a number of years although it is not specifically referred to in the Data Protection Act. The concept involves a senior official in an organisation suspected of a data protection breach accepting that there has been a violation of the statutory requirements and undertaking to take specified steps both to terminate the breach and to minimise the possibility of it occurring again. Such an event might well trigger further and more formal enforcement procedures. Perhaps the most relevant undertaking was sought and obtained from NHS Digital in respect of its failure to observe patient's declared wishes to opt out of various forms of data sharing. This was considered by the Commissioner to constitute a breach of the first data protection principle relating to the fair and lawful processing of personal data. Following discussions, measure were agreed to rectify matters and an undertaking given as to this. To date, there has been no reported case of a failure to comply with an undertaking, but if this were to occur it could result in more formal enforcement procedures with the breach serving as an aggravating factor in determining the size of any financial penalty or other sanction that might be imposed upon an organisation.

d. Formalities prior to processing: the general regime under the current framework

Is there a regime requiring the fulfilment of certain conditions prior to any processing activities different from that applicable to research in the field of health? If yes, what does that regime entail?

Conditions relating to processing are common across all forms of processing requiring that details of the processing be notified to the Information Commissioner. No special provision is made for health data or indeed for any other form of data. In general, although it requires to be made prior to the commencement of processing, notification is a formal step and there is no provision for it to be rejected. Section 22 of the Act does make provision for the Information Commissioner to conduct a preliminary assessment of the legality of proposed processing. To date, however, it does not appear that this power has been exercised in any case although it is of course possible that information supplied during the notification process may serve as the basis for future enforcement actions.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

3. Further processing of health data (for research purposes): the current regime

How is the notion of further processing regulated in your national framework?

The second data protection principle in the 1998 Act requires that:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

A controller will be required to specify the forms of processing which will be undertaken – including the range of persons to whom the data might be disclosed or transferred – and thereafter restrict processing to these areas of activity.

Are there specific conditions to the further processing for scientific research in the field of health purposes?

There are no health specific conditions relating to further processing. There is an ongoing debate when techniques of anonymization or the use of pseudonyms might suffice to separate data from a linkage with identifiable individuals and thereby take it outside the category of personal data.

What are the rights of the data subject when it comes to further processing?

In interpreting the first data protection principle, Schedule one of the 1998 Act provides that:

2.—(1) … or the purposes of the first principle personal

data are not to be treated as processed fairly unless—

(a) in the case of data obtained from the data subject, the data controller

ensures so far as practicable that the data subject has, is provided with,

or has made readily available to him, the information specified in subparagraph

(3), and

(b) in any other case, the data controller ensures so far as practicable that,

before the relevant time or as soon as practicable after that time, the

data subject has, is provided with, or has made readily available to him,

the information specified in sub-paragraph (3).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

The "relevant time" is essentially the time at which personal data is first processed. In the case where personal data is transferred to another party for further processing, there will be obligation on this party to inform the data subject and either seek consent or indicate reliance on one of the other statutory factors that may justify processing.

What about the data subject's rights and further processing for scientific research purposes?

4. The GDPR's impact on the current regulatory framework for the processing of health data for research purposes

a. The impact of the GDPR on the rules applying to processing for research in the field of health

Please provide a summary of the main relevant characteristics of the new law/Bill (as far as it is relevant for processing health data for research purposes). How is (or will be) Article 9(2)(j) implemented in your country?

Article 9(2)(j) provides that the general prohibition against the processing of sensitive personal data (the special categories) may not be applied where:

"processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

In implementing this provision, the Bill provides that:

2 (1) This condition is met if the processing is necessary for health or social care purposes.

(2) In this paragraph "health or social care purposes" means the purposes of—

(a) preventive or occupational medicine,

(b) the assessment of the working capacity of an employee,

(c) medical diagnosis,

(d) the provision of health care or treatment,

(e) the provision of social care, or

(f) the management of health care systems or services or social care systems or services.

(3) See also the conditions and safeguards in Article 9(3) of the GDPR

(obligations of secrecy) and section 11(1) (of the Bill).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

11 Special categories of personal data etc: supplementary

(1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a) by or under the responsibility of a health professional or a social work professional, or

(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

10. Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

(a) point (b) (employment, social security and social protection);

(b) point (g) (substantial public interest);

(c) point (h) (health and social care);

(d) point (i) (public health);

(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(6) The Secretary of State may by regulations—

(a) amend Schedule 1—

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

(i) by adding or varying conditions or safeguards, and

(ii) by omitting conditions or safeguards added by regulations

under this section, and

(b) consequentially amend this section.

b. Modification to the processing authorisation procedure applying to research in the field of health

How will the processing authorisation procedure (if any exists) be affected by the implementation of the GDPR? Can you describe any such change?

What about the right of the data subject and the obligations of the controller?

102 Each controller must implement appropriate measures—

(a) to ensure, and

(b) to be able to demonstrate, in particular to the Commissioner,

that the processing of personal data complies with the requirements of this

Part.

103 Data protection by design

(1) Where a controller proposes that a particular type of processing of personal

data be carried out by or on behalf of the controller, the controller must, prior

to the processing, consider the impact of the proposed processing on the rights

and freedoms of data subjects.

(2) A controller must implement appropriate technical and organisational

measures which are designed to ensure that—

(a) the data protection principles are implemented, and

(b) risks to the rights and freedoms of data subjects are minimised.

103 (1) If a controller becomes aware of a serious personal data breach in relation to

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

personal data for which the controller is responsible, the controller must notify the Commissioner of the breach without undue delay.

(2) Where the notification to the Commissioner is not made within 72 hours, the notification must be accompanied by reasons for the delay.

(3) Subject to subsection (4), the notification must include—

(a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) the name and contact details of the contact point from whom more information can be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

129 Consensual audits

(1) The Commissioner's functions under Article 58(1) of the GDPR and paragraph 1 of Schedule 13 include power, with the consent of a controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice in the processing of personal data.

(2) The Commissioner must inform the controller or processor of the results of such an assessment.

(3) In this section, "good practice in the processing of personal data" has the same meaning as in section 128.

10 Special categories of personal data etc: supplementary (1) For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy)

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

include circumstances in which it is carried out— (a) by or under the responsibility of a health professional or a social work professional, or (b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

5. Further processing for research purposes under the GDPR

The notion of further processing under the GDPR:

How to measure the compatibility of purpose of the further processing:

The particularities of scientific research: a presumption of purpose compatibility

Given the regime applied to further processing in the GDPR, can you describe the consequences, if any, in your national legal framework?

Data relating to health will require to be processed in accordance with the requirements of Schedule One of the Bill relating to special categories of data. Section 10 of the Bill provides for the processing of personal data relating to "health and social care. The Bill adopts the GDPRs definition of health data. The Information Commissioner has commented that

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

The Bill continues to establish the conditions that must be satisfied in order for the processing of sensitive data to be lawful. It states that this will be permitted when the processing is "necessary" for the purposes of

(a) preventive or occupational medicine,

(b) the assessment of the working capacity of an employee,

(c) medical diagnosis,

(d) the provision of health care or treatment,

And continues to make reference to the requirement that processing should comply with:.

the conditions and safeguards in Article 9(3) of the GDPR (obligations of secrecy) and section 11(1).

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Section 11(1) requires that the processing should take place under the control of a health professional or (and rather more vaguely "by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law".

6. Health data sources for research purposes

a. Sources of data and their regulation

Does your national framework contain specific provisions for anonymised or pseudonymised health data?

No specific provisions apply.

What are the different sources of health data that can be used for research purposes?

- **DIRECT COLLECTION FROM PATIENTS:**

Under the current legal framework: please explain the currently applying rules that a researcher, who intends to collect health data directly from individuals (e.g. via a survey, or by asking patients to wear a monitoring device, etc.), should follow.

The collection of health data directly from a patient will undoubtedly constitute the processing of sensitive data. Such processing is lawful only if it complies with the data protection principles and at least one of the conditions in each of Schedules 2 and 3 of the Act is satisfied.

The first data protection principle requires that data be processed fairly and lawfully. In determining whether data is processed fairly, Schedule One of the Act requires that where data is obtained from a data subject, the subject is informed at the time in question of the identity of the data controller and of the purpose(s) for which the data will be processed.

Schedule 3 provides for a number of factors legitimising processing. These include that the subject has consented to the processing. The term consent is not defined in the Act but professional rules established by bodies such as the General Medical Council place considerable emphasis on the need for patient consent to be informed in nature. Schedule 3 also legitimised processing in the absence of consent where this is necessary for medical purposes and is undertaken by a health professional or by a person who is subject to an obligation of confidence equivalent to that which will be owed to the patient by the health professional.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

No changes of substance may be anticipated when the GDPR and Data Protection Act 2018 enter into force. Some requirements, however, are specified in greater clarity and detail than has been the case under the 1998 Act. Consent will remain a basis legitimising processing with Section 84 of the Act providing the definition that consent:

in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

Schedule 8 of the Act enacts a number of other factors that may serve to legitimise the processing of sensitive data and is couched in essentially the same terms as the 1998 legislation; allowing for processing where it is

necessary for medical purposes and is undertaken by—

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality

which is equivalent to that which would arise if that person were a

health professional.

The term "medical purposes" is defined as including "the purposes of preventative

medicine, medical diagnosis, medical research.. (and) .. the provision of care and treatment".

- **COLLECTION FROM HEALTH PROFESSIONALS AND HEALTH INSTITUTIONS**

Under the current legal framework: please explain the rules currently applying that a researcher, who intends to obtain health data from medical staff, hospitals, etc., should follow.

Under the 1998 Act, the party acquiring personal data will fall to be classed as a data controller in their own right. They will be obliged to notify details of the proposed processing to the Information Commissioner and comply with the provisions of the Act. In the case of health data, there may also be professional requirements that the researcher will be obliged to comply with,

Under the revised legal framework: Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

There will be no significant changes under the new regime

.

- **PRIVATE DATABASES**

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

Under the current legal framework: please explain the rules currently applying for the setting up of and the use of a private database with health data for research purposes.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

No special rules apply in respect of the establishment of private data bases. The general provisions of the Data Protection Act will apply regarding notification prior to the commencement of processing and to the requirement to comply with the data protection rules regarding processing of sensitive personal data. Any relevant professional rules will also be required to be complied with.

The new legal framework will not change this situation to any significant extent. The ICO will receive some increased powers to intervene to assess the legality of processing although in many instances these can be exercised at least initially only on a consensual basis. The level of monetary penalties that may be imposed on a data controller in the event of any breach of the Act's principles has been increased.

- **PUBLIC DATABASES**

Under the current legal framework: do public authorities make available health data for research purposes in your country and under what conditions?

NHS Digital, described above, is charged with the duties of supplying:

information and data to the health service, (it) provides vital technological infrastructure, and helps different parts of health and care work together.

Information may also be made available to other undertakings and organisations under the Data Access Request Service. A register of approved data releases is maintained by NHS digital and is a publicly available document.

Under the revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

No changes appear to be planned for the operation of the system under the new data protection regime.

b. Application of the national framework to the AEGLE cases

1. Type 2 diabetes

The AEGLE project uses, after pseudonymisation, health data collected from patients who have expressed their consent with their data being used further for research purposes.

- Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' _analytics on the AEGLE platform? Is a new ethical or other approval required? From which body? Should

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

the patient be informed about the new research project? Is a new patient consent, specifically focusing on the precise research project, required?

The question whether pseudonymous data falls to be considered as personal data is critical in this context. In determining whether data is identifiable, the 1998 Act states in section 1 that account is to be taken of "those data and other information which is in the possession of, or is likely to come into the possession of, the data controller".

The reliance on subject consent should serve to legitimize processing but there may be a question whether this is sufficiently full or informed.

- Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

The major change that may be anticipated is the introduction of a few definition regarding the issue of identifiability. The Act incorporates the definitional provisions of the GDPR but does not itself provide a definition of "pseudonymisation'". Section 171, however, provides that

(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject

2. Intensive Care Unit (ICU)

AEGLE uses data generated by ICU devices without collecting the patient's consent (after pseudonymisation). Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' _analytics on the AEGLE platform? Is a new ethical or other type of approval required? From which body? Should the patient be informed about the new research project?

The initial collection of the personal data may well be justified by the statutory ground of necessity. The fact of processing will require to be notified to the ICO but no particular difficulties might be envisaged.

Further issues will arise in respect of the transfer of data for research purposes. The Act requires that where personal data is transferred for further processing that the data subject has to be informed of the purpose to which it will be put. This presupposes that the data involved falls within the definition of personal data, i.e. whether it relates to identifiable individuals.

Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

The general principles to be applied will be much the same although it may be that more extensive steps will have to be taken to ensure that the patient has full knowledge of the additional purposes to which the data will be put

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU

3. Chronic Lymphocytic Leukaemia (CLL)

The AEGLE project re-uses, after pseudonymisation, data coming from biobanks. In this instance, patients have given their informed consent for the samples and for the processing of their data. But this consent was given in general terms and not specifically for AEGLE.

Current legal framework: which procedural or other steps would the researcher have to follow to use this data for 'big data' _analytics on the AEGLE platform? Is a new ethical or other approval required? From which body? Should the patient be informed about the new research project?

Once again, the degree of anonymity conferred upon individual patients' data will be a factor that requires to be taken into account. If the pseudonymisation process is effective, the data will fall outside the scope of the Data Protection Act, although its use may still require the approval of professional ethics bodies. This presupposes that consent is sufficient. Processing of personal data begins at the moment when data is collected and the level of consent given at that time will influence the legality of further processing.

Revised legal framework: will the currently existing procedures and rules change in view of the implementation of the GDPR in your country?

The major change that might be envisaged is the strengthening of requirements for consent. Subject to the issue how anonymous data might be, implementation of the GDPR is likely to require more in the way of consent to specific forms of processing than has hitherto been the case.

Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 644906.

Partners
EXUS AE (Coordinator), ICCS, KINGSTON, CERTH, Maxeler Technologies Limited, UPPSALA UNIVERSITET, UNISR, time.lex, EUR, CHS, LOBA, PAGNI, GNUBILA FRANCE, NTU